



A REPORT  
TO THE  
MONTANA  
LEGISLATURE

INFORMATION SYSTEMS AUDIT

# *Policy Holder System*

## *Montana State Fund*

NOVEMBER 2007

LEGISLATIVE AUDIT  
DIVISION

07DP-14

**LEGISLATIVE AUDIT  
COMMITTEE**

**REPRESENTATIVES**

BILL BECK  
BILL GLASER  
BETSY HANDS  
HAL JACOBSON, VICE CHAIR  
JOHN SINRUD

**SENATORS**

JOE BALLYEAT, CHAIR  
GREG BARKUS  
STEVE GALLUS  
DAVE LEWIS  
LYNDA MOSS  
MITCH TROPILA

**AUDIT STAFF**

**INFORMATION SYSTEMS**  
NATHAN TOBIN

FRAUD HOTLINE  
HELP ELIMINATE FRAUD,  
WASTE, AND ABUSE IN  
STATE GOVERNMENT. CALL  
THE FRAUD HOTLINE AT:

(STATEWIDE)  
1-800-222-4446  
(IN HELENA)  
444-4446

**INFORMATION SYSTEM AUDITS**

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:  
Legislative Audit Division  
Room 160, State Capitol  
PO Box 201705  
Helena MT 59620-1705  
(406) 444-3122

Reports can be found in electronic format at:  
<http://leg.mt.gov/audit.htm>

# LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor  
Tori Hunthausen,  
Chief Deputy Legislative Auditor



Deputy Legislative Auditors:  
James Gillett  
Angie Grove

November 2007

The Legislative Audit Committee  
of the Montana State Legislature:

We conducted an Information Systems audit of the Policy Holder System (PHS). Montana State Fund (MSF) operates and maintains the PHS to assist in the administration of workers' compensation policy holder records and premiums. The focus of the audit was to determine whether the PHS was operating as expected in its primary functions of maintaining policy holder records, calculating policy holder premiums, and processing policy holder premium payments.

This report contains two recommendations for the development and implementation of review procedures to ensure coverage levels are current in the PHS and excessive user access to the PHS is identified and removed.

We wish to express our appreciation to MSF for their cooperation and assistance.

Respectfully submitted,

*/s/ Scott A. Seacat*

Scott A. Seacat  
Legislative Auditor

## TABLE OF CONTENTS

Figures and Tables .....	ii
Appointed and Administrative Officials .....	iii
Executive Summary .....	S-1
<b>CHAPTER I — INTRODUCTION AND BACKGROUND .....</b>	<b>1</b>
Introduction .....	1
Audit Objectives .....	1
Audit Scope and Methodology .....	1
<b>CHAPTER II — POLICY HOLDER PREMIUM RATES.....</b>	<b>3</b>
Introduction .....	3
PHS Calculating Premiums .....	3
PHS Edits Require Necessary Policy Information to be Entered .....	4
MSF Accurately Loading Premium Rates in PHS .....	4
MSF Not Loading Coverage Rates in PHS.....	5
<b>CHAPTER III — PREMIUM PAYMENTS AND TRANSACTIONS .....</b>	<b>7</b>
Introduction .....	7
PHS Process Creating Invoices.....	8
Premium Payment Transaction File Complete and Accurate .....	8
<b>CHAPTER IV — POLICY HOLDER SYSTEM ACCESS .....</b>	<b>9</b>
Introduction .....	9
MSF Deactivates Accounts of Terminated Users .....	9
Users with Incompatible Access.....	9
Unauthorized Users with Ability to Create Transactions .....	10
Generic Accounts Preventing Accountability .....	10
Excessive Users with Access to Source Code .....	10
Summary .....	11
<b>AGENCY RESPONSE .....</b>	<b>A-1</b>
Montana State Fund.....	A-3

# FIGURES AND TABLES

## Figures

Figure 1	Policy Holder System Data Flow .....	7
----------	--------------------------------------	---

## Tables

Table 2	Examples of Premium Rates for Different Business Types .....	4
---------	--	---

## APPOINTED AND ADMINISTRATIVE OFFICIALS

### Montana State Fund

Laurence Hubbard, President/CEO

Al Parisian, CIO

Patti Grosfield, Internal Auditor

## EXECUTIVE SUMMARY

Montana State Fund (MSF) is as a non-profit, publicly owned, workers' compensation insurance carrier established by Title 39, Chapter 71, of Montana Code Annotated (MCA). MSF provides optional worker's compensation insurance for approximately 25,000 Montana employers. MSF is self-funded through revenues obtained from employer premium payments, and is governed by a seven member board of directors appointed by the Governor.

As the primary workers' compensation carrier in Montana, both employers and employees rely heavily on MSF for their coverage. Montanan employers who choose MSF as their workers' compensation carrier are considered policy holders. Each policy holder is required to pay an annual premium amount based on the type of business they operate and the amount of their annual payroll. By paying the premium, the policy holders ensure compensation for their employees injured while on the job.

To assist in the administration of policy holder accounts and premium payments, MSF maintains and operates a computer system called the Policy Holder System (PHS). MSF uses the PHS to assist in the administration of policy holder accounts and billing. The scope of this audit involved testing system controls in place to ensure the PHS was operating as expected in its primary functions of maintaining policy holder records.

The report contains two recommendations for the development and implementation of review procedures to ensure coverage levels are current in the PHS and excessive user access to the PHS is identified and removed.

.





# Chapter I — Introduction and Background

## **Introduction**

Montana State Fund (MSF) is a workers' compensation insurance carrier established by Title 39, Chapter 71, of Montana Code Annotated (MCA). MSF provides worker's compensation insurance for approximately 30,000 Montana employers. MSF is self-funded through revenues obtained from employer premium payments, and is governed by a seven member board of directors appointed by the Governor.

As the primary workers' compensation carrier in Montana, both employers and employees rely heavily on MSF for their coverage. Montana employers who choose MSF as their workers' compensation carrier are considered policy holders. Policy holders are required to pay an annual premium amount based on the type of business they operate and the amount of their annual payroll. By paying the premium, policy holders ensure compensation for their employees injured while on the job. During fiscal year 2006, MSF collected approximately \$212 million in premium payments from policy holders, and \$142 million was paid out in past and current fiscal year claims.

To assist in the administration of policy holder accounts and premium payments, MSF maintains and operates a computer system called the Policy Holder System (PHS). Since premium payments fund MSF operations, it is critical to employers and employees throughout the state payments are calculated and processed in an accurate and complete manner.

## **Audit Objectives**

This information systems audit focused on PHS operations including processing policy holder records, premium amounts, and premium payments. Based on the importance of PHS in the management of policy holder accounts, we addressed the following objectives:

- ♦ Verify the PHS is accurately and completely uploading and calculating premium rates for Policy Holders.
- ♦ Verify the PHS is accurately and completely processing premium payment transactions.

## **Audit Scope and Methodology**

MSF relies on the PHS to calculate policy holder rates and process premium payments. Through interview and review of PHS functionality, we identified these as the primary and critical functions of the PHS. Therefore, the scope of this audit focused on these functions and the controls MSF has in place to ensure they work as expected.

Testing of PHS functionality and controls was conducted through a combination of staff interviews, observation of PHS processes, and extraction and analysis of PHS data using a computer-assisted audit tool.

This audit was conducted in accordance with Government Auditing Standards published by the United States General Accountability Office (GAO). We evaluated the control environment using state law and generally applicable and accepted information technology standards established by the IT Governance Institute.

## Chapter II — Policy Holder Premium Rates

### **Introduction**

State law (39-71-401, MCA) requires most employers to provide workers' compensation coverage for their employees in the event they are involved in an on-the-job accident. To obtain coverage, an employer must submit an application to become a policy holder. Once accepted, the new policy holder will have their business' information entered into the PHS. Using this information, the PHS calculates the premium amount owed by the policy holder to MSF to maintain coverage for their employees. The PHS uses a combination of factors to determine what a policy holder will owe, including:

- ♦ Policy holder annual payroll;
- ♦ Class code rates determined by type of business the policy holder is involved in; and,
- ♦ Experience modifiers based on the policy holders' safety records and business safety programs.

Our audit work addressed PHS processes involved in calculating premiums and testing was done to ensure these processes are accurately calculating premium amounts owed. The tests conducted for this section are as follows:

- ♦ Determine PHS process responsible for calculating premium amounts is referring to appropriate data fields.
- ♦ Ensure PHS has edits in place to ensure all required policy holder data is entered.
- ♦ Ensure updated premium rates are accurately and completely loaded in the PHS.

### **PHS Calculating Premiums**

Payments are calculated from a policy holder's annual payroll, their class code rate, and experience modifiers. The manual premium is the result of the rate applied to the policy holder's annual payroll. To determine if the PHS is calculating premium amounts as expected, we reviewed the programming code responsible for this process to ensure all necessary components are being included in the calculation. Through our review, we were able to identify references to data fields containing payroll amount, class rates, and experience modifiers. Based on this, and our professional judgment, we can make a reasonable conclusion the PHS process is functioning as expected.

## **PHS Edits Require Necessary Policy Information to be Entered**

When a new policy holder record is created in the PHS, it is necessary to include certain information to be able to identify the policy holder and for the PHS to calculate an accurate premium amount, including, but not limited to:

- ♦ Name of business
- ♦ Address of business
- ♦ Class code
- ♦ Covered Employees
- ♦ Estimated Payroll
- ♦ Policy Holder Role

Audit work was done to ensure the above sets of data are entered in the PHS every time a new policy holder account is created. MSF represents the PHS has edits in place forcing the user creating the new account to enter the required information. Edits are components of a system that notify a user when a required field of data has not been entered and will not allow the record to be saved until all required fields are entered. We observed the creation of a policy holder account in the PHS to ensure edits notify the user a required field has not been entered and to prevent the user from saving the record if any of the required fields are left blank. Through this observation, we conclude edits are in place to require all necessary information to create a policy holder account and calculate a premium payment.

## **MSF Accurately Loading Premium Rates in PHS**

Each policy holder is assigned a class code identifying the type of business. Each class code has rates assigned to them, and the rate amount depends on the risk of accident associated with the type of business. For example, generally a job in construction is at a higher risk for an on-the-job accident than a clerical job. Therefore, policy holders whose employees hold high-risk jobs will pay higher premium rates than policy holders whose employees work in lower-risk fields. The class rate is the percentage of a company's payroll that will determine their premium amount. Each year these rates are adjusted and approved by the board of directors at MSF. All new rates affecting policy holder premium calculation are to be loaded into the PHS prior to July 1 of each year. Table 2 provides examples of rates for different business types.

**Table 2**  
**Examples of Premium Rates for Different Business Types**

<b>Business Type</b>	<b>Base Class Code Rate</b>
Clerical	.97
Roofing	54.06
Taxidermist	5.37
Surface Coal Mining	5.01
Underground Coal Mining	39.85

**Source: Compiled by the Legislative Audit Division from information provided by Montana State Fund's Fiscal Year 2007 Underwriting Manual.**

In conjunction with the class code rates, there are additional rates affecting what some policy holders may pay in premiums. One of these rates is a construction industry premium credit, which provides a premium discount to policy holders in the construction business.

To ensure MSF is accurately loading the new rates into the PHS prior to July 1, 2007, we compared the rates in the PHS database to the actual rates approved by the board of directors. This comparison was conducted in August of 2007. Following the comparison, we were able to conclude all class code and construction industry premium credit rates in the PHS reflected the rates approved by the board of directors.

### **MSF Not Loading Coverage Rates in PHS**

In a typical workers' compensation coverage policy only employees are covered, so MSF offers an elective coverage for owners who also wish to be covered. Each year new coverage levels are issued which dictate the minimum and maximum a policy holder will pay if they elect to provide themselves with workers compensation coverage. Coverage levels must be loaded to the PHS by July 1.

Our testing showed the current year coverage levels associated with the elected owner coverage had not been updated for the current Fiscal Year. MSF relies on a manual upload of these levels into the PHS but has no controls to ensure the manual process occurred or worked. As a result, they were unaware the owner levels had not been updated until we notified them.

The unchanged levels only affect the maximum a policy holder will pay, and since very few policy holders pay the maximum amount for this type of coverage, MSF represents no policies were effected. However, without controls in place to ensure current levels have been uploaded, there is existing potential policy holders may not be paying the accurate amount owed on their premiums. Since MSF was notified their coverage levels were not current, they have updated those levels.

---

#### **RECOMMENDATION #1**

*We recommend the department develop and implement controls to ensure coverage levels in the PHS are current.*

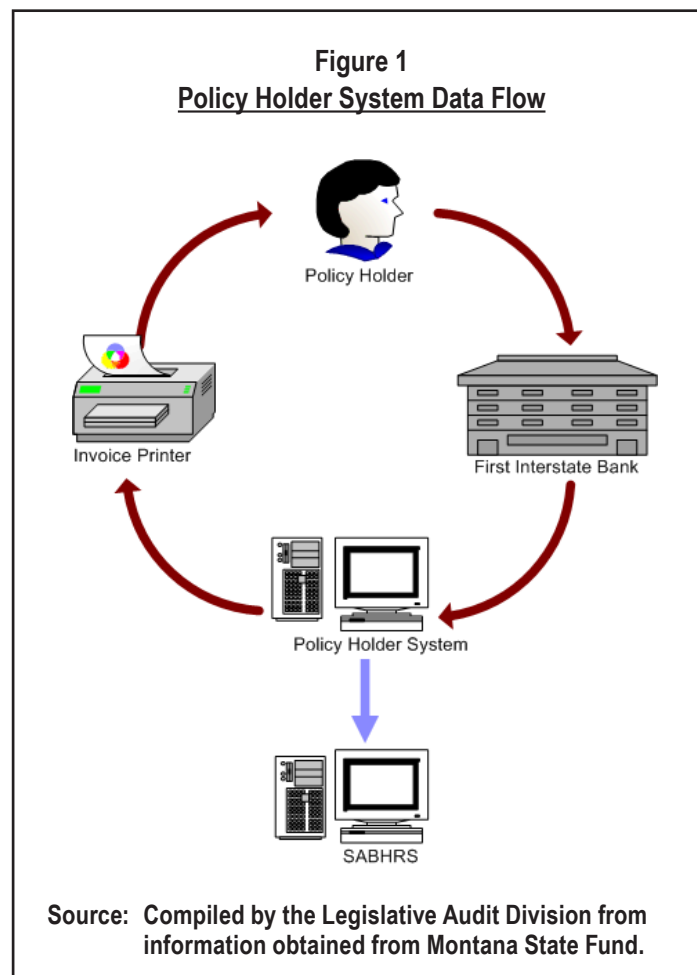
---



## Chapter III — Premium Payments and Transactions

### Introduction

Once a premium amount is determined, it is the responsibility of the policy holder to pay the amount. Depending on the policy holder's preference and the amount of the premium, they can pay on an annual, quarterly, or monthly basis. To provide the policy holder with their current payment status and amount owed, the PHS automatically creates invoices when payment is due. When a policy holder receives the invoice, they have 25 days to make payment. Premium payments are typically sent to the First Interstate Bank in Billings where each payment is compiled into a computer file. This file is sent to MSF on a nightly basis and the payment records are loaded into the PHS. The premium payment records are then transferred from the PHS to the state's accounting system, SABHRS. Figure 1 below illustrates the data flow for this process.



Our audit work addressed PHS premium billing and payment operations, and testing was done to ensure the PHS is accurately creating premium invoices and processing premium payments. The following sections describe testing we conducted:

- ♦ Determine PHS process responsible for creating premium invoices refers to appropriate data fields.
- ♦ Ensure PHS has edits in place to ensure transaction records sent from First Interstate Bank to MSF are complete and accurate.

### **PHS Process Creating Invoices**

When a new policy holder applies for coverage, they can choose the date they would like to be billed. The date is entered into the policy holder's record in the PHS. Other data necessary to create an invoice include policy holder identification, policy identification, a valid address, and amount due. To determine if the PHS is accurately printing invoices, we reviewed the programming code responsible for this process to ensure all of necessary data fields are referenced. Through our review, we were able to identify functions that:

- ♦ Check for valid addresses.
- ♦ Identify the invoice date each month.
- ♦ Insert policy ID, policy holder ID, and balance amount into appropriate table.
- ♦ Send invoice to be printed in nightly batch.

Based on audit work, we conclude functions necessary to process an invoice are present in the programming code, and the PHS process creating automated invoices is working as expected.

### **Premium Payment Transaction File Complete and Accurate**

On a nightly basis, a transaction file is sent from First Interstate Bank in Billings to MSF where it is loaded in the PHS. To ensure each transaction record is transferred in a complete and accurate manner, edits have been implemented through the PHS to prevent the transfer until certain requirements are met. MSF expects the following from each transaction record:

- ♦ Each transaction record must have a unique identifier.
- ♦ The policy holder number must be valid.
- ♦ The amount of funds transferred must be in a numeric format.

To verify edits exist to ensure a complete and accurate file load to MSF, we reviewed the script code responsible for processing the transaction to ensure above transaction requirements are addressed. Through our review, we conclude MSF has controls in place to ensure an accurate and complete transfer.



## Chapter IV — Policy Holder System Access

### **Introduction**

The PHS operates through interaction with PHS users who are MSF staff with a business need to access the system. To gain access to the PHS, MSF security staff must assign a unique login ID to each potential user. Furthermore, based on the type of job the user is assigned, access needs to be limited to tasks specific to their job. This is accomplished by assigning each user security roles, which dictate what screens in the PHS a user has access to and whether they can update, create, delete, or just view data. MSF is also responsible for limiting those with access to the internal components of the PHS, including programming code and database tables. To ensure MSF is limiting user access to appropriate levels, we tested to ensure the following:

- ◆ Terminated employees do not have active access to the PHS.
- ◆ User security roles coincide with their job roles.
- ◆ MSF is limiting access to production code and database tables to knowledgeable staff with a business need for this access.

### **MSF Deactivates Accounts of Terminated Users**

When an employee leaves a position at MSF, their user accounts should be deactivated. Otherwise, the threat exists a disgruntled former employee can make unauthorized changes, resulting in damage to the integrity of the system or loss of sensitive data. We compared active user accounts in the PHS system with a list of terminated state employees in the state's accounting and human resource system, SABHRS. We found MSF has deactivated all terminated employee user accounts.

### **Users with Incompatible Access**

When users have incompatible access, the potential increases unauthorized alteration or theft of sensitive data can occur. MSF represented they are preventing this by establishing what rights each job type should have in the system and creating a security role. They state they will only assign the security role that matches a user's job title. However, we reviewed the access list to the PHS and identified the following exceptions:

- ◆ Two users with access roles that do not match their job duties.
- ◆ The security officer responsible for assigning user access has been granted five different access roles, of which two do not correspond with assigned job duties.

## **Unauthorized Users with Ability to Create Transactions**

The PHS can be used to create payments in the form of refunds and credits to a policy holder. The ability to create refund and credit transactions should be limited to accounting staff. However, our review of the PHS access list shows 19 users who are not accounting staff with the ability to create a transaction, including information technology staff and various supervisors. Testing found none of these users have created an unauthorized transaction, but the potential is magnified with so many having the access to do so.

## **Generic Accounts Preventing Accountability**

We also tested to determine if MSF was using generic accounts to provide access. Generic accounts are a risk because they are not assigned to a single user and are often used by multiple users. As a result, the potential exists the generic accounts could be used for unauthorized activity in the PHS and the user responsible could not be identified. Our review found two active generic accounts in the MSF access list. MSF management represents these account are not being used and should have been removed. Since being notified of their existence, the accounts have been deactivated. Through further testing, we were able to confirm there were not unauthorized transactions created using these accounts.

## **Excessive Users with Access to Source Code**

The production environment is where the operating version of a system is stored. Included in the environment is programming code and database tables. Access to the production system should be limited to those whose job duties require the ability to work with these components. Otherwise, the potential exists unauthorized changes can be made to code or database tables changing the functionality of the system. Additionally, the threat of manipulation, loss, and theft of sensitive data increases.

We reviewed the list of users with access to source code and database tables in the production environment and found 13 users with access to source code and two users with access to the database tables. Further review identified the two users with access to the database tables were acceptable. We also found seven of the 13 users with access to source code to be valid. However, six of the 13 users with access to the source code do not require it. We also found these users are allowed this access by sharing a single administrative account allowing this access. Because all these users share the same user ID, a single user cannot be held accountable in the event an unauthorized change is made to the production environment.

## **Summary**

MSF management has been notified of these exceptions and were unaware they existed. At the time of the audit, MSF did not have procedures or policies in place to review and analyze PHS access for inappropriate access and user accountability. Currently, they are in the process of developing review procedures to identify these types of exceptions. They have also removed the excessive access we identified.

---

### **RECOMMENDATION #2**

*We recommend the department develop review procedures to identify and remove inappropriate access, including:*

- A. Users whose access is not required of their job duties;*
  - B. Generic accounts; and,*
  - C. Users with unnecessary access to the production environment.*
-

MONTANA STATE  
FUND

AGENCY RESPONSE



5 South Last Chance Gulch • P.O. Box 4759 • Helena, MT 59604-4759  
 Customer Service: 1-800-332-6102 or 406-444-6500  
 Fraud Hotline: 1-800-682-7463 (800-MT-CRIME)

November 9, 2007

Mr. Scott A. Seacat  
 Legislative Audit Division  
 Room 160, State Capitol  
 PO Box 201705  
 Helena, MT 59620-1705

RECEIVE

NOV 13 2007

LEGISLATIVE AUDIT DIV.

Re: MSF response to LAD Information Systems audit of the Policy Holder System (PHS)

Dear Mr. Seacat:

Following is our response to the items identified as recommendations in the recent Legislative Audit Division audit report related to our PHS policy system.

LAD Recommendation #1: "We recommend the department develop and implement controls to ensure coverage levels in the PHS are current."

**MSF Response:**

The first recommendation in the audit relates to optional Owner/Officer payroll minimum and maximum coverage levels. Each year, these coverage levels normally increase for cost of living and the levels are provided to us externally by the Department of Labor. These levels are then loaded into our QA system and tested. Once testing is approved, they are loaded into our production environment. This year, the process proceeded as normal; however, this particular update did not get committed to our production system so the levels did not load.

**MSF Control Action:**

In order to eliminate this problem in the future, we will be making a change to our change management system to provide for an automated final review of production data. The final step will be required in order for the change request to be closed. This will apply to all of our change requests. Our business analyst will need to review each change request that was applied to production for each build and verify that it is actually in the production environment. Once this is determined the business analyst will close the change request. This will provide one final review in the process to ensure that all change requests have been properly applied. If it is determined that a particular change request did not get committed to production, our change request manager can complete an emergency fix and ensure that it is in. This new process will be implemented by December 31, 2007.

LAD Recommendation #2: "We recommend the department develop review procedures to identify and remove inappropriate access, including:

- A. Users whose access is not required of their job duties;
- B. Generic accounts; and,
- C. Users with unnecessary access to the production environment.

**MSF Response:**

This recommendation deals with our policy holder system access. Contained within the above LAD Recommendation #2 A,B,C, are four areas where concerns from LAD were noted. They are more specifically stated by LAD as follows:

- A1. Users with incompatible access. Two users with access roles that do not match their job duties, and the security officer has two roles that do not correspond with her assigned duties.
- A2. Unauthorized users with ability to create transactions.
- B. Generic accounts preventing accountability.
- C. Excessive users with access to source code.

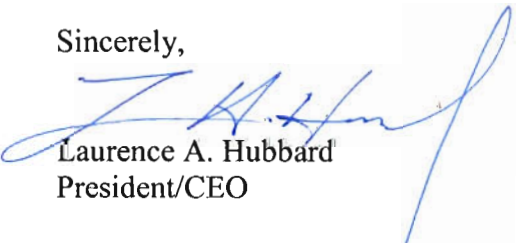
**MSF Control Action:**

- A1. The internal auditor will work with MSF management/leaders to review 1) the access roles of the two users indicated that may not match their job duties, and 2) the security officer's two roles in question. This will be completed and changes deemed necessary by management will be made by December 31, 2007.
- A2. The internal auditor will work with MSF management/leaders to determine appropriate roles for these users. Two of the identified unauthorized users have already been removed (8/31/2007). Review of the rest will be completed by December 31, 2007, and changes deemed necessary by management will be made.
- B. The internal auditor will work with MSF management/leaders to determine the need for any generic accounts. Those not valid will be removed. The review and any changes deemed necessary by management will be completed by December 31, 2007.
- C. The internal auditor will work with MSF management/leaders to determine proper 'policy type' security roles to be assigned to the six PHS system users mentioned. Any security role changes needed will then be implemented by December 31, 2007.

Overall, a formal periodic review process will be created to ensure the security roles, authorities and access are maintained at the appropriate levels. This formal process will occur periodically and include a formal listing transmitted to the MSF leadership and the internal auditor for their review.

Montana State Fund appreciates the efforts and professionalism exhibited by the audit staff involved in this review of our policy holder system (PHS). Thank you for the opportunity to respond to the recommendations made by your auditors.

Sincerely,



Laurence A. Hubbard  
President/CEO

LAH/pg